Georgia State University Policy

7.20.16 University Information Systems Use

Policy Summary

All approved university policies that are aimed at ensuring the access, use and protection of information systems are summarized here. This policy’s scope, terms, compliance and violations sections apply to all the information systems policies listed here.

Full Policy Text

Georgia State University’s information systems are critical resources and play an integral part in the fulfillment of the university’s objectives of teaching, research and extension of knowledge to the public. The Georgia State University Information Systems Use Policies provide guidelines for the access, use and protection of these resources.

Scope

This document and the catalogued policies apply to students, and all university employees, including, but not limited to, faculty and staff. The policies also apply to all individuals, whether authorized or not, who use the university’s information systems from any location. Use of the university’s information systems, even when carried out on a privately owned computer that is not managed or maintained by the university, is governed by these policies.

Compliance

Violations of these policies may result in the discipline of an individual in accordance with applicable University policies or state or federal law, including criminal prosecution. The university may temporarily suspend, block or restrict access to Information Systems when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Information Systems or to protect the university from liability.

Reporting Violations

Alleged violations of the policies should be reported to the appropriate university disciplinary and/or law enforcement authorities. If the alleged violation could pose a security hazard to the university’s technology resources, the alleged violation should also be reported to the university’s Information Security Officer for appropriate action to secure the affected technology resources. When appropriate, the university disciplinary and/or law enforcement authorities will coordinate with the university’s Information Security Officer to investigate and respond to alleged violations. Alleged violations of policies will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff and students, as outlined in the Faculty Handbook, the Student Code of Conduct, and other applicable policies and procedures.

Appeals
Users found in violation of any of the catalogued policies may appeal any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

**Administrative Procedures**
This document and any of the catalogued policies may be changed by the Information Technology Senate Sub-Committee (ITSS), with such changes being reviewed and recommended through the Senate Information Systems and Technology Committee (ISAT). Information Systems and Technology (IS&T) will prepare, coordinate and process all recommended changes.

**Policies**
Following are the current Information System Use Policies in practice at Georgia State University.

**Information System Use Policies**

**Policy**
**What is it?**What do is apply to?What needs to be done?**

- **Anti-virus Software Policy**
  - Requires mandatory use of anti-virus protection for Windows and Macintosh computers
  - Anyone at Georgia State with a personal computer connected to the university network
  - Install a copy of university-provided anti-virus software; see the Procedures section for download and installation directions

- **Computer Accounts Policy**
  - Describes the basic requirements and expiration rules for university computer accounts
  - Anyone at Georgia State using the university’s computing and networking resources
  - Understand the basic requirements and expiration rules for university computer accounts

- **Digital Monitors for Public Display**
  - Digital signage systems are an integral component of branding, public image, and emergency communications; therefore, these monitors must conform to university standards related to information security, management systems, and network standards
  - Anyone who has installed or is planning to install a digital monitor device
  - Read the policy and follow the outlined standards and procedures

- **E-mail Directory Policy**
  - A single directory of official institutional e-mail addresses is maintained, and any requirement for official institutional email addresses must use this singular source
  - Anyone at Georgia State who needs official institutional e-mail addresses
  - Use the university’s Campus Directory to obtain official institutional e-mail addresses

- **E-mail System Acceptable Use and Security Policy**
  - Describes how university e-mail systems will be managed and protected
  - Anyone at Georgia State who uses e-mail
  - Use strong passwords; do not send confidential information via email; follow procedures to send e-mail messages to large numbers of Georgia State recipients

- **Graham-Leach-Bliley Act and the FTC Safeguards Rule: GSU Information Security Plan**
  - Every University department that handles or maintains customer information is responsible for identifying the type of information, the form of the information and the security risks within their department and taking appropriate measures to mitigate those risks
  - Departments at Georgia State that handle or maintain customer information
  - Read the policy and follow the outlined standards and procedures

- **Incident Response Policy**
  - Information Security incidents occurring on the university network or attached devices will be managed centrally by the University Information Security Officer (ISO) and will include other campus resources as determined by the ISO
  - Anyone at Georgia State
  - Read the policy and follow the outlined standards and procedures

- **Information Systems Ethics Policy**
  - Requires appropriate and civil use of network resources; describes institutional protection of
Information Protection and Access Policy

Describes how university data and information should be accessed and protected. Anyone at Georgia State that utilizes or accesses university data and information should be protected according to its definition level of confidential, sensitive or unrestricted.

Information Security Management System (ISMS) Requirements (ISO 27001) as a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

All University personnel are responsible for the security and privacy of the data they access, transmit, and store as prescribed in University policy, legal, regulatory, and statutory requirements.

Corrective Action Procedure

Internal Audit Procedure

Preventive Action Procedure

Minimum Information Security Environment Policy

Minimum precautions for securing computing devices and access to the Georgia State network. Responsibilities of the Information Security Officer:

- Anyone at Georgia State using computers or having responsibility for a server:
  - Don’t use computers or systems you are not authorized to use;
  - Don’t send an e-mail as if you were someone else;
  - Use the university-supported versions of Windows, Mac OS, and Novell; Netware, GroupWise, VPN (Virtual Private Network) and anti-virus clients;
  - Follow the password generation rules for creating passwords;
  - Don’t share userids and passwords;
  - Maintain documentation to verify proper licensing of purchased software;
  - Physically protect your computer or server;
  - Do not attempt to defeat the security of information systems.

Network Connection of Surveillance System Cameras and Digital Video Recorders Policy

Approval and configuration requirements for video systems used to protect resources or personnel:

- Anyone at Georgia State planning to install a digital surveillance system:
  - Contact the Information Security Officer prior to acquisition and installation.

Remote Access Policy

Off-campus access to network and systems are through approved methods only:

- Anyone at Georgia State providing access to local servers from off-campus locations:
  - Anyone accessing a Georgia State network or information system from off-campus:
    - Read the policy and follow the outlined standards and procedures.
    - Use a Virtual Private Network (VPN) client for authentication and encryption; see Procedure for details.

Security Review Policy

Where appropriate, Information Security personnel will conduct risk assessments of technologies/processes that are being evaluated and/or used at Georgia State University:

- Anyone at Georgia State:
  - Read the policy and follow the outlined standards and procedures.

Web Accessibility Policy

This policy assures that university web-based materials are available to all who attempt to access them:

- Anyone who develops, manages or writes content for a gsu.edu website:
  - Develop Web sites and on-line courses in compliance with the Priority One elements of the W3C guidelines (http://www.w3.org/WAI) or exceed them.

Web Policy

Georgia State’s Web sites will exhibit a uniform and cohesive identity through the use of the approved content management system (CMS):

- College, Academic Department and Administrative Web sites:
  - Web sites for student organizations are not produced within the CMS.
  - At this time, individual faculty pages are not required to be developed in the CMS.

All Georgia State University World Wide Web publishers must comply with the guidelines described in this document.

Wireless Access Policy

WiFi/802.11 access through centrally managed authenticated methods:

- Anyone using a wireless device at Georgia State:
  - Anyone installing a wireless access point on Georgia State’s network
Administration of Policy

Mandating Authority:
Administrative Council

Responsible Office(s):
Information Systems and Technology, 13th floor, Commerce Building, 3-4357

Responsible Executive(s):

Policy History

Approving Body: Administrative Council

Rationale or Purpose

The purpose of this document is to summarize and provide in a single location all approved policies aimed at ensuring that the access, use and protection of the information systems promote the university’s objectives. These policies will achieve the following principles:

- ensure that users abide by state and federal laws, as well as the policies of the university and the University System of Georgia;
- ensure that all individuals accessing or using the information systems assume responsibility for protecting these resources from unauthorized access, modification, destruction or disclosure;
- ensure the integrity, reliability and availability of the information systems; and
- ensure that individuals do not abuse the university’s information systems and do respect the rights of members of the university community.

Additional Information

Additional Helpful Resources